Secure Authentication from a Weak Key, Without Leaking Information

Niek J. Bouman and Serge Fehr
Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands.
{n.j.bouman,serge.fehr}@cwi.nl

Abstract

We study the problem of authentication based on a weak key in the information-theoretic setting. A key is weak if its min-entropy is an arbitrary small fraction of its bit length. This problem has recently received considerable attention, with different solutions optimizing different parameters. We study the problem in an extended setting, where the weak key is a one-time *session key* that is derived from a public source of randomness with the help of a (potentially also weak) *long-term* key. Our goal now is to authenticate a message by means of the weak session key in such a way that (nearly) no information on the long-term key is leaked. Ensuring privacy of the long-term key is vital for the long-term key to be re-usable. Previous work has not considered such a privacy issue, and previous solutions do not seem to satisfy this requirement.

We propose a new four-round protocol for message authentication. The session key that is used to perform authentication is allowed to be weak. Given a secure look-ahead extractor, we prove that our protocol satisfies *security* against an active adversary and *long-term-key privacy*, which means that the protocol avoids significant information leakage about the long-term key. For the setting where the adversary's side information about the session key is classical, we can use an existing construction for a secure look-ahead extractor. For the general case, in which this side information is a quantum state, we were not able to show the existence of a secure look-ahead extractor, and leave this as an open problem.

NJB is supported by an NWO Open Competition grant.

Contents

1 Introduction

We consider the problem of message authentication based on a *weak key* over a public channel that might be under the control of an active adversary. A key is *weak* if its min-entropy is an arbitrary small fraction of its bit length. We study this problem in the information-theoretic setting, i.e. we assume the adversary to be computationally unbounded.

In a setting where a sender transmits a message to a receiver, the goal of *message authentication* is to convince the receiver that the received message is identical to the transmitted message, i.e. that it has not been modified by an adversary during transmission. A related problem that can also be solved by message authentication is where the sender has not transmitted any message, but the adversary injects a message into the channel instead.

For information-theoretically secure authentication, the sender and receiver need to share a common secret key K. To authenticate a message m using the classic approach for message authentication [CW77], the sender computes a *tag* $T := f(K, m)$, where f is some function, and sends the tag T along with the message. Note that the function f

is usually called *message authentication code* (MAC). The receiver then applies f to K and the received message m' and compares this with the tag. For the classic approach to be secure, the authentication key needs to be *strong* (unformly distributed), and may generally be used only once.

As mentioned above, we consider a scenario where the key is *weak*. Because we are dealing with an *active* adversary, the standard approach of using a randomness extractor to turn the weak key into a strong one (which can then be used to perform standard message authentication) will *not* work, since the adversary can tamper with the extractor's seed.

Specifically, we consider the following scenario. Alice and Bob share a *long-term* key W. When needed, Alice and Bob can extract a weak *session key* X_W from an auxiliary source of randomness with the help of W. It should be guaranteed by the property of the auxiliary source that a potential adversary Eve who does not know W has limited information on the weak session key X_W. This is formalized by requiring that $H_{\min}(X_W|WE) \geq k$ for some parameter k, where E denotes Eve's side information. This scenario occurs naturally in e.g. Maurer's *bounded-storage model* [Mau90], where W determines which part of the huge string to read, as well as in the quantum setting, where W determines in which basis to measure some quantum state.

The goal is to authenticate a message μ from Alice to Bob with the help of the weak session key X_W, while guaranteeing *security*, in that if Eve tampers with μ then this will be detected, and *privacy*, in that Eve cannot learn information about the long-term key W. We stress that the privacy property is vital for Alice and Bob to be able to re-use W. Note that once Alice and Bob can do message authentication with a weak key, then they can also do key agreement, simply by doing standard randomness extraction where the seed for the extractor is communicated in an authentic way.

We want to emphasize that, by assumption, every new session key X_W for the same long-term key W contains fresh randomness, provided by the auxiliary source. Therefore, the goal above does not contradict the well-known impossibility result of re-using an authentication key without refreshing. Also note that we do not specify how exactly the auxiliary source of randomness produces X_W from W; on the contrary, we want security no matter how X_W is obtained, as long as X_W contains enough min-entropy (given the adversary's information and W).

1.1 Related Work

With regard to the security property from above, the problem of authentication from a weak key in the presence of an active adversary is a fairly well-studied problem. On the contrary, and to the best of our knowledge, we are the first to study the special case where the weak key is obtained from a long-term key and where privacy of the long-term key needs to be guaranteed. In particular, the works that we will mention below do not address this case, and moreover they all fail to satisfy the privacy property.

In the following discussion, let n be the bitsize of the key (in our case, the session key) and k its min-entropy (in bits). It was proved by Dodis and Wichs [DW09] that non-interactive authentication is impossible when $k \leq n/2$, even when the parties have access to local non-shared randomness, which we will assume. For a good overview of earlier work on the case where $k > n/2$, we refer to [DW09].

The first protocol for interactive authentication from arbitrarily weak keys is due to Renner and Wolf [RW03]. It requires $\Theta(\ell)$ rounds of interaction to authenticate an ℓ-bit message. In [DW09], an authentication protocol from arbitrarily weak keys is described that

only needs two rounds of interaction, which is optimal (in terms of the number of rounds). Chandran *et al.* [CKOR10] focus on minimizing entropy loss and describe a privacy amplification protocol that is optimal with respect to entropy loss (up to constant factors). Their construction needs a linear number of rounds (linear in the security parameter).

The case where Alice and Bob share highly-correlated, but possibly unequal keys—the "fuzzy" case—is addressed in [RW04] and improved upon by Kanukurthi and Reyzin [KR09], but also covered by [DW09] and [CKOR10].

1.2 Motivation

The main motivation for the work in this chapter comes from *password-based identification* in the bounded-quantum-storage model (BQSM). Damgård *et al.* [DFSS07] propose two identification protocols: `QID`, which is only secure against dishonest Alice or Bob, and $\texttt{QID}^+$, which is also secure against a man-in-the-middle (MITM) attack. However, only `QID` is truly password-based; in $\texttt{QID}^+$, Alice and Bob, in addition to the password, also need to share a high-entropy key.

Now, the observation is that with the help of an authentication protocol with long-term-key privacy, the protocol $\texttt{QID}^+$ can be turned into a truly password-based identification protocol in the BQSM with security against MITM attacks.

Based on $\texttt{QID}^+$, Damgård *et al.* also propose an *authenticated* quantum key distribution protocol in the BQSM, which, in contrast to standard quantum key distribution protocols, does not require authenticated communication but has the authentication "built in." Furthermore, in contrast to using standard quantum key distribution in combination with standard authentication, in the authenticated quantum key distribution protocol the authentication keys can be re-used. By making $\texttt{QID}^+$ truly password-based, Damgård *et al.*'s authenticated QKD protocol will become truly password-based as well.

1.3 Contributions

We propose a new four-round protocol for message authentication with a weak session key X_W. The protocol is an extension of the two-round protocol by Dodis and Wichs [DW09], which is based on *look-ahead extraction*. Given a secure look-ahead extractor, we prove that our protocol satisfies *security* and *long-term-key privacy*, meaning that the adversary Eve cannot tamper with the authenticated message without being detected, nor does she learn a non-negligible amount of information on the long-term key W.

For the case where Eve's side information about X_W is classical, we can use the construction for a look-ahead extractor that is given in [DW09]. Contrary to what we have claimed in [BF11] (see Section 6.2 for a more detailed explanation), it remains an open problem to construct a look-ahead extractor that is secure against quantum side information, or, to prove that the construction given in [DW09] (which is secure in the presence of classical side information) is also secure against quantum side information. Hence, we cannot yet construct an authentication protocol that is secure in the quantum setting, which would be needed for our envisioned application, i.e. truly password-based identification in the BQSM with security against MITM attacks.

1.4 The Fuzzy Case

We will also discuss the "fuzzy case," i.e. where there are some errors between Alice's and Bob's weak session key. If Eve's side information is classical, then our techniques are known to be secure in the fuzzy case; in the quantum setting, however, this remains to be shown. Precisely this latter case—the quantum setting—is relevant for our password-based-identification application.

2 Notation and Preliminaries

We prove security of our scheme in the presence of a *quantum* adversary with *quantum* side information, and below we introduce some suitable notations. However, we stress that most of the notation and the proofs can also be understood from a purely classical information-theoretical point of view.

The *state* of a quantum system X is given by a *density matrix* ρ_X, i.e., a positive-semidefinite trace-1 matrix acting on some Hilbert space $\mathcal{H}_X$. We denote the set of all such matrices, acting on $\mathcal{H}_X$, by $\mathcal{P}(\mathcal{H}_X)$. In the special case where ρ_X is diagonal, X is called *classical*, and in this case we can understand X as a random variable, where its distribution P_X is given by the diagonal entries of ρ_X. In this case, we tend to slightly abuse notation and write $X \in \mathcal{X}$ to indicate that the range of the random variable X is $\mathcal{X}$.

If X is part of a bi-partite system XE, then X is called classical if the density matrix ρ_{XE} of XE is of the form $\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_{E|X=x}$, where P_X is a probability distribution, $\{|x\rangle\}_x$ forms an orthonormal basis of $\mathcal{H}_X$, and $\rho_{E|X=x} \in \mathcal{P}(\mathcal{H}_E)$. In this case, X can be understood as random variable, and system E is in state $\rho_{E|X=x}$ exactly if X takes on the value x. We therefore sometimes also speak of a random variable X and a quantum system E. To simplify notation, we often write ρ_E^x instead of $\rho_{E|X=x}$. Readers that are unfamiliar with quantum information can safely think of E as being classical as well, in which case the $\rho_{E|X=x}$'s are all diagonal, with the probabilities of the conditional distributions $P_{E|X}(\cdot|x)$ as diagonal entries.

The distance between two states $\rho_X, \sigma_X \in \mathcal{P}(\mathcal{H}_X)$ is measured by their *trace distance* $\frac{1}{2}\|\rho_X - \sigma_X\|_1$, where $\|\cdot\|_1$ is the L_1 norm.[1] In case of classical states, i.e., ρ_X and σ_X correspond to distributions P_X and Q_X, the trace distance coincides with the statistical distance $\frac{1}{2}\sum_x |P_X(x) - Q_X(x)|$.

We write $x \xleftarrow{R} \mathcal{X}$ to denote that the element x is picked independently and uniformly at random from the set $\mathcal{X}$. $\mathbb{N}$ denotes the set of strictly positive integers. For any $n \in \mathbb{N}$, we write $[n]$ for the set $\{1, \ldots, n\}$. $\mathbb{F}_q$, $\mathbb{F}_q^*$ denote respectively the finite field of order $q \in \mathbb{N}$, where $q = p^n$ for p a prime and $n \in \mathbb{N}$, and the multiplicative group of $\mathbb{F}_q$. In particular, $\mathbb{F}_2 := (\{0,1\}, \oplus, \cdot)$, where $\oplus$ and $\cdot$ respectively denote addition and multiplication modulo 2. We also use $\oplus$ and $\cdot$ to denote addition and multiplication in $\mathbb{F}_2$ extension fields. Furthermore, we use the $\oplus$ symbol for vector addition in an $\mathbb{F}_2$ vector space.

In the following definitions, we consider a bi-partite system XE with classical X. X is said to be *random and independent* of E if $\rho_{XE} = \rho_U \otimes \rho_E$, where ρ_U is the fully mixed state on $\mathcal{H}_X$ (i.e., U is classical and - as random variable - uniformly distributed). In case of classical E, this is equivalent to $P_{XE} = P_U \cdot P_E$ (in the sense that $P_{XE}(x,e) = P_U(x) \cdot P_E(e)$ $\forall x, e$). The following definition measures how far away XE is from such an ideal situation.

[1] Defined by $\|A\|_1 := \mathrm{trace}(\sqrt{A^\dagger A})$, where $A^\dagger$ denotes the Hermitian transpose.

Definition 1 (Distance to Uniform)**.** The *distance to uniform* of X given E is defined as

$$d(X|E) := \tfrac{1}{2}\|\rho_{XE} - \rho_U \otimes \rho_E\|_1.$$

If also E is classical, then $d(X|E)$ simplifies to

$$d(X|E) = \tfrac{1}{2}\sum_{x,e} |P_{XE}(x,e) - P_U(x)P_E(e)| = \sum_e P_E(e)\,\tfrac{1}{2}\sum_x \big|P_{X|E}(x|e) - P_U(x)\big|.$$

It is not too hard to show that for a tri-partite system XYE with classical X and Y

$$d(X|YE) = \sum_{y\in\mathcal{Y}} P_Y(y)\, d(X|E, Y{=}y).$$

From this, the following lemma follows immediately.

Lemma 2. *For any y: $d(X|E, Y{=}y) \le d(X|YE)/\Pr[Y = y]$.*

Definition 3 (Guessing Probability)**.** The *guessing probability* of X given E is defined as

$$p_{\mathsf{guess}}(X|E) := \sup_{\{M_x\}_x} \sum_x P_X(x)\mathrm{tr}(M_x\,\rho_E^x),$$

where the supremum is over all POVMs $\{M_x\}_x$ on $\mathcal{H}_E$.

In case also E is classical, $p_{\mathsf{guess}}(X|E)$ simplifies to the standard average guessing probability

$$p_{\mathsf{guess}}(X|E) = \sum_e P_E(e)\max_x P_{X|E}(x|e).$$

Definition 4 (Min-Entropy)**.** The min-entropy of X given E is defined as

$$H_{\min}(X|E) := -\log p_{\mathsf{guess}}(X|E).$$

This definition coincides with the definition introduced by Renner [Ren05], as shown by [KRS09]; in case of a classical E, it coincides with the definition of *average* conditional min-entropy (see e.g. [DORS08]).

Definition 5. A function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k,ε)-strong extractor, if for any bipartite quantum system XE with classical X and with $H_{\min}(X|E) \ge k$, and for a uniform and independent seed Y, we have

$$d\big(\mathsf{Ext}(X,Y)\big|YE\big) \le \varepsilon\,.$$

Note that we find "extractor against quantum adversaries" a too cumbersome terminology; thus we just call Ext a (strong) extractor, even though it is a stronger notion than the standard notion of a (strong) extractor. When necessary, we distinguish between the two notions by saying that an extractor is or is not *secure against quantum side information.*

A well-known example of a strong extractor (that is secure against quantum side information) is a two-universal hash function $h : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^q$. Indeed, for any XE with classical X, and for Y an independent seed, uniformly distributed on $\{0,1\}^d$ privacy amplification [RK05] guarantees that

$$d(h(X,Y)|YE) \le \frac{1}{2}\sqrt{2^{q-H_{\min}(X|YE)}} = \frac{1}{2}\sqrt{2^q\, p_{\mathsf{guess}}(X|YE)}.$$

2.1 Security Definition

In this paper, an *authentication protocol* is understood as a classical protocol between two parties Alice and Bob. Alice inputs a message μ and a weak session key X_W, and Bob inputs a message μ' and the same session key X_W. At the end of the protocol, Bob announces a Boolean decision whether to "accept" or "reject." The weak session key X_W may depend arbitrarily on a long-term key W. During the execution of the protocol, an adversary Eve has full control over the communication between Alice and Bob.

We require the protocol to fulfill the following formal definition.

Definition 6. Let $E_\circ, E$ denote Eve's respective a priori and a posteriori quantum systems, where the latter includes Bob's decision on whether to accept or reject. A $(n, k, m, \delta, \varepsilon)$ message-authentication protocol with long-term-key privacy is defined to satisfy the following properties:

1. Correctness If there is no adversary Eve present, then for any message $\mu \in \{0,1\}^m$ and $\mu' = \mu$, and for any (distribution of the) key $X_W \in \{0,1\}^n$, Bob accepts with certainty.
2. Security If $H_{\min}(X_W|WE_\circ) > k$, then for any $\mu, \mu' \in \{0,1\}^m$ with $\mu \neq \mu'$, the probability that Bob accepts is at most δ.
3. Long-Term-Key Privacy If $\rho_{WE_\circ} = \rho_W \otimes \rho_{E_\circ}$ and $H_{\min}(X_W|WE_\circ) > k$, then

$$\frac{1}{2}\|\rho_{WE} - \rho_W \otimes \rho_E\|_1 \leq \varepsilon\,.$$

3 Dodis and Wichs' Authentication Protocol

In this section, we describe a slightly modified version of the two-round message-authentication protocol due to Dodis and Wichs [DW09]. We will use this protocol later as a "starting point" to construct our message-authentication protocol. We start by giving a few definitions that are crucial for the understanding of the protocol by Dodis and Wichs.

Definition 7 (Epsilon Look-Aheadness)**.** Let t, ℓ be positive integers. Let $A := (A_1, \ldots, A_t)$ and $B := (B_1, \ldots, B_t)$ be random variables over $(\{0,1\}^\ell)^t$, and let E be a quantum system. For all $i \in \{0, \ldots, t-1\}$ let ε_i be defined as

$$\varepsilon_i := d_{\text{unif}}\big(A_{i+1} \ldots A_t \big| B_1 \ldots B_i E\big)\,.$$

The ordered pair (A, B) is *ε-look-ahead conditioned on E* if $\varepsilon \geq \max_i \varepsilon_i$.

Definition 8 (Look-Ahead Extractor)**.** $\mathsf{laExt} : \{0,1\}^n \times \{0,1\}^d \to (\{0,1\}^\ell)^t$ is called a *(k, ε)-look-ahead extractor* if for any random variable $X \in \{0,1\}^n$ and quantum system E with $H_{\min}(X|E) \geq k$ the following holds. Let $S \in \{0,1\}^d$ be an independent and uniformly distributed seed, and let $\tilde{S} \in \{0,1\}^d$ be adversarially chosen given S and E; this may involve a (partial) measurement of E, resulting in the new state E'. Then, the ordered pair $(R, \tilde{R})$ where $R = (R_1, \ldots, R_t) := \mathsf{laExt}(X; S)$ and $\tilde{R} = (\tilde{R}_1, \ldots, \tilde{R}_t) := \mathsf{laExt}(X; \tilde{S})$ is ε-look-ahead conditioned on S, $\tilde{S}$ and E'.

Informally, a look-ahead extractor has the property that even if the adversary is allowed to modify the seed, when given the first i blocks of the key that is extracted using the modified seed, the remaining blocks of the key that is extracted using the correct seed still look random.

Definition 9 (Look-Ahead-Secure MAC)**.** A family of functions

$$\{\mathsf{MAC}_\kappa : \{0,1\}^m \to \{0,1\}^s\},$$

indexed by keys $\kappa \in (\{0,1\}^\ell)^t$ is an (ε, δ) *look-ahead-secure* MAC if for any pair of fixed and distinct messages $\mu_\mathrm{A}, \mu_\mathrm{B} \in \{0,1\}^m, \mu_\mathrm{A} \neq \mu_\mathrm{B}$, and any ordered pair of random variables $(K, K') \in (\{0,1\}^\ell)^{2t}$ satisfying the look-ahead property with parameter ε conditioned on quantum system E,

$$p_{\mathsf{guess}}\big(\mathsf{MAC}_K(\mu_\mathrm{B}) \,\big|\, \mathsf{MAC}_{K'}(\mu_\mathrm{A})E\big) < \delta\,.$$

We are now ready to present the Dodis and Wichs message-authentication protocol `DWMAC`. The protocol we present here is slightly modified in that we assume that Alice has already sent her message μ_A to Bob, who has received it as μ_B (possibly $\neq \mu_\mathrm{A}$). This modification is for simplicity, and because we do not aim at minimizing the number of rounds. X_W is the weak key, known to both Alice and Bob. The function $\mathsf{laExt} : \{0,1\}^n \times \{0,1\}^d \to (\{0,1\}^\ell)^t$ is a (k, ε)-look-ahead extractor and $\mathsf{MAC}_\kappa : \{0,1\}^m \to \mathbb{F}_{2^s}$ is a (ε, δ) look-ahead-secure MAC.[2]

Protocol `DWMAC`: When Alice wants to authenticate the message μ_A to Bob, then *Bob* first sends a random seed R to Alice, upon which Alice replies with the tag T_A.

Alice(X_W, μ_A)		Bob(X_W, μ_B)
		$R \xleftarrow{\mathrm{R}} \{0,1\}^d$
	$\xleftarrow{R}$	
$K := \mathsf{laExt}(X_W; R)$		$K := \mathsf{laExt}(X_W; R)$
$T_\mathrm{A} := \mathsf{MAC}_K(\mu_\mathrm{A})$		$T_\mathrm{B} := \mathsf{MAC}_K(\mu_\mathrm{B})$
	$\xrightarrow{T_\mathrm{A}}$	
		accept if: $T_\mathrm{A} = T_\mathrm{B}$
		else: abort

Security of `DWMAC` follows immediately from the definitions of the underlying building blocks: laExt ensures that Alice and Bob's versions of the key K satisfy the look-ahead property, and in this case it is guaranteed that MAC acts as a secure MAC, even when Alice's key was modified.

However, in our setting where we additionally want to maintain privacy of the long-term key W, which may arbitrarily depend on X_W, `DWMAC` does not seem to be good enough, unless Eve remains passive. Indeed, if Eve does not manipulate the communicated seed R, then by the assumed lower bound on $H_{\min}(X_W|WE)$ it follows that the extracted K on Bob's side is close to random and independent of W (and E), and thus T leaks no information on W. However, if Eve manipulates the seed R (for instance replaces it by a value of her choice), then there is no guarantee anymore that K, and thus T, does not leak information on W.

Another and more subtle way for Eve to (potentially) learn information on W is by not manipulating the message, i.e., have $\mu_\mathrm{A} = \mu_\mathrm{B}$, but manipulate the seed R and try to obtain information on W by observing if Bob accepts or not.

[2] It will become clear later why we require the range of the MAC to be the field $\mathbb{F}_{2^s}$. Note that by fixing a basis for this field, we can associate every vector in $\mathbb{F}_2^s$ with a unique field element in $\mathbb{F}_{2^s}$, and *vice versa*. Hence, via this induced vector-space isomorphism, MAC_κ is an instance of Definition 9. Finally, we want to emphasize that this vector-space isomorphism $\mathbb{F}_2^s \to \mathbb{F}_{2^s}$ is not a natural one; it depends on the chosen basis.

3.1 Towards Achieving Key-Privacy

We give here some intuition on how we overcome the above privacy issues of DWMAC with respect to the long-term key W. Similarly to our notation T_{A} and T_{B} to distinguish between the tag computed by Alice and by Bob, respectively, we write R_{A} and R_{B} etc. to distinguish between Alice and Bob's values of R etc., which may be different if Eve actively manipulates communicated messages.

A first approach to prevent leakage through T_{A} is to one-time-pad encrypt T_{A}. Let $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^k \to \mathbb{F}_{2^s}$ a strong extractor (since we merely give a high-level explanation here, we do not specify all parameters of this extractor here). The key for the one-time pad is extracted by means of a strong extractor Ext from X_W, where Alice chooses the seed:

Alice		Bob
	$\xleftarrow{R}$	
$S \xleftarrow{\mathrm{R}} \{0,1\}^k$		
$Z := \mathsf{Ext}(X_W; S)$		
$Q := T_{\mathrm{A}} \oplus Z$	$\xrightarrow{S, Q}$	
		$Z := \mathsf{Ext}(X_W; S)$
		accept if: $Q = T_{\mathrm{B}} \oplus Z$

In the above protocol (and also below), we understand T_{A} and T_{B} to be computed as in DWMAC. Note that since it is Alice who chooses the seed S and since $H_{\min}(X_W|WE)$ is lower bounded, Z_{A} is guaranteed to be (close to) random and independent of W (and E), and thus hides all information that T_{A} might leak on W. However, this modification renders the *security* of the protocol invalid. For instance, we cannot exclude that by modifying the seed S appropriately, Eve can enforce $Z_{\mathrm{B}} = T_{\mathrm{B}}$, so that she only needs to send $Q = 0$ to have Bob convinced.

In order to restore security while still preventing information to leak through T_{A}, we let Bob choose a random non-zero "multiplier" for the one-time pad key Z:

Alice		Bob
	$\xleftarrow{R}$	
$S \xleftarrow{\mathrm{R}} \{0,1\}^k$		$C \xleftarrow{\mathrm{R}} \mathbb{F}^*_{2^k}$
$Z := \mathsf{Ext}(X_W; S)$		
	$\xrightarrow{S}$	
	$\xleftarrow{C}$	
abort if $C = 0$		
$Q := T \oplus C \cdot Z$	$\xrightarrow{Q}$	
		$Z := \mathsf{Ext}(X_W; S)$
		accept if: $Q = T_{\mathrm{B}} \oplus C \cdot Z$

Leakage through T_{A} is still prevented since a non-zero multiple of a good one-time-pad key is still a good one-time-pad key. Furthermore, for security, we can intuitively argue as follows. Consider a snapshot of an execution of the protocol after S has been communicated. We give Eve the value T_{A} for free; this only makes her stronger. By the security of the underlying DWMAC protocol, we know that it is hard for Eve to guess T_{B}. Now, assuming that there exist two distinct values for C for which Eve can predict the corresponding value $Q_{\mathrm{B}} = T_{\mathrm{B}} \oplus C \cdot Z_{\mathrm{B}}$, it follows immediately that Eve can actually predict T_{B}; a contradiction. Hence, there can be at most one value for Bob's choice of C for which Eve can guess Q_{B} reasonably well.

We point out that the above intuitive reasoning involves *rewinding*; this is fine in the classical setting, but fails when quantum information is involved due to no-cloning (see e.g. [VDG98]). Thus, in our formal security proof where we allow Eve to maintain a quantum state, we have to reason in a different way. As a consequence, in the actual protocol, Q is computed in a slightly different way.

One issue that we have not yet addressed is that Bob's decision to accept or reject may also leak information on W when $\mu_{\mathrm{A}} = \mu_{\mathrm{B}}$ and Eve modifies one (or both) of the seeds R and S. Note that this is not an issue if $\mu_{\mathrm{A}} \neq \mu_{\mathrm{B}}$ because then, by the security property, Bob rejects with (near) certainty. For instance it might be that changing the first bit of S changes Z or not, depending on what the first bit of X_W is. Thus, by changing the first bit of S and observing Bob's decision, Eve can learn the first bit of X_W, which may give one bit of information on W. The solution to overcome this problem is intuitively very simple: we use MAC not only to authenticate the actual message, but also to authenticate the two seeds R and S. Then, like in the case $\mu_{\mathrm{A}} \neq \mu_{\mathrm{B}}$, if Eve changes one of the seeds then Bob's will reject. Note that this modification introduces a circularity: the key K, which is used to authenticate the seed R (as well as the message and S) is extracted from X_W by means of the seed R. However, it turns out that we can deal with this.

4 Our Construction

We now turn to our construction for the message-authentication protocol with long-term-key privacy (Definition 6). Let $\mathsf{laExt} : \{0,1\}^n \times \{0,1\}^d \to (\{0,1\}^\ell)^t$ be a (k_K, ε_K) look-ahead extractor. Let $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^v \to \mathbb{F}_{2^q}$ be a (k_Z, ε_Z)-strong extractor. Let $\mathsf{MAC} : (\{0,1\}^\ell)^t \times (\{0,1\}^m \times \{0,1\}^d \times \{0,1\}^v) \to \mathbb{F}_{2^s}$ be a $(\epsilon, \lambda + \epsilon)$ look-ahead-secure MAC for any $\epsilon > 0$. Let X_W be the session key, shared among Alice and Bob, and satisfy $H_{\min}(X_W|WE_\circ) \geq \max(k_K + q, k_Z)$, and recall from Definition 6 that $E_\circ$ denotes Eve's a priori quantum system. For all $n \in \mathbb{N}$ where $n \geq 1$ and all $t \in [n]$ we let

$$[\cdot]_t : \mathbb{F}_{2^n} \to \mathbb{F}_{2^t}$$

be an arbitrary but fixed linear surjective function.

Protocol `AUTH` is shown below.

In Section 6, we show how to instantiate the building blocks to obtain a protocol with reasonable parameters that can be used in a scenario where Eve has classical side information. For the quantum setting, we cannot yet instantiate protocol `AUTH`: we currently do not have a construction for a look-ahead extractor that is provably secure against quantum side information.

Depending on the parameters of an instantiation of `AUTH` and on the bitsize of μ_{A}, it might be better (or even necessary) to authenticate a hash of the tuple (μ_{A}, R, S), instead of authenticating the tuple itself. In this case, we let Alice choose a small seed for an almost universal hash function and apply MAC_K to this seed and the hash of the the tuple (μ_{A}, R, S) (with respect to this seed). We will actually make use of this idea in Section 6.

Before going into the security proof for protocol `AUTH`, we resolve here the circularity issue obtained by authenticating the seed R that was used to extract the authentication key K.

Lemma 10. *Consider a family of functions MAC_κ (indexed by keys $\kappa \in (\{0,1\}^\ell)^t$) that is a $(\xi, \lambda + \xi)$-look-ahead-secure MAC for any ξ. Let K, K', M_{A} and M_{B} be arbitrary random variables and E a quantum state, and let the ordered pair $(K, K') \in (\{0,1\}^\ell)^{2t}$*

Protocol $\texttt{AUTH}\,(X_W, \mu_\mathrm{A}; X_W, \mu_\mathrm{B})$

$\mathrm{Alice}(X_W, \mu_\mathrm{A})$		$\mathrm{Bob}(X_W, \mu_\mathrm{B})$
		$R \xleftarrow{\mathrm{R}} \{0,1\}^d$
	$\xleftarrow{R}$	
$K := \mathsf{laExt}(X_W; R)$		$K := \mathsf{laExt}(X_W; R)$
$S \xleftarrow{\mathrm{R}} \{0,1\}^v$		
	$\xrightarrow{S}$	
$Z := \mathsf{Ext}(X_W; S)$		$Z := \mathsf{Ext}(X_W; S)$
$T_\mathrm{A} := \mathsf{MAC}_K((\mu_\mathrm{A}, R, S))$		$T_\mathrm{B} := \mathsf{MAC}_K((\mu_\mathrm{B}, R, S))$
		$U \xleftarrow{\mathrm{R}} \mathbb{F}_{2^s}, V \xleftarrow{\mathrm{R}} \mathbb{F}^*_{2^q}$
	$\xleftarrow{U,V}$	
if $V = 0$: abort		
$Q := [U \cdot T_\mathrm{A}]_q \oplus V \cdot Z$		
	$\xrightarrow{Q}$	
		accept if: $Q = [U \cdot T_\mathrm{B}]_q \oplus V \cdot Z$
		else: abort

satisfy the look-ahead property with parameter ε conditioned on M_A, M_B, E and the event $M_\mathrm{A} \neq M_\mathrm{B}$. Then,

$$p_{\mathsf{guess}}\big(\mathsf{MAC}_K(M_\mathrm{B}) \,\big|\, \mathsf{MAC}_{K'}(M_\mathrm{A}) M_\mathrm{A} M_\mathrm{B} E, M_\mathrm{A} \neq M_\mathrm{B}\big) < \lambda + t\varepsilon.$$

Note that in the lemma above the messages may depend on the keys, whereas Definition 9 considers *fixed* messages.

Proof. We condition on $M_\mathrm{A} = m_\mathrm{A}$ and $M_\mathrm{B} = m_\mathrm{B}$ where $m_\mathrm{A} \neq m_\mathrm{B}$. Because (K, K') may depend on $(M_\mathrm{A}, M_\mathrm{B})$, conditioning on fixed values for the latter implies that (K, K') is not necessarily ε-look-ahead anymore. Let $\varepsilon_{m_\mathrm{A}, m_\mathrm{B}}$ be the maximum over $i \in [t]$ of the following expression,

$$\varepsilon_{m_\mathrm{A}, m_\mathrm{B}, i} := d_{\mathrm{unif}}(K_{i+1} \ldots K_t \big| K'_1 \ldots K'_i E, M_\mathrm{A} = m_\mathrm{A}, M_\mathrm{B} = m_\mathrm{B}).$$

Hence, by Definition 7, (K, K') is $\varepsilon_{m_\mathrm{A}, m_\mathrm{B}}$-look-ahead conditioned on E and the events $M_\mathrm{A} = m_\mathrm{A}$ and $M_\mathrm{B} = m_\mathrm{B}$. Note that averaging $\varepsilon_{m_\mathrm{A}, m_\mathrm{B}, i}$ over m_A and m_B (conditioned on them being distinct) results in

$$\varepsilon_i = d_{\mathrm{unif}}(K_{i+1} \ldots K_t | K'_1 \ldots K'_i M_\mathrm{A} M_\mathrm{B} E, M_\mathrm{A} \neq M_\mathrm{B}\big) \leq \varepsilon\,.$$

Furthermore, note that by conditioning on fixed and distinct values for M_A and M_B, we fulfill the requirements for MAC look-ahead security from Definition 9. I.e. we can conclude that

$$p_{\mathsf{guess}}\big(\mathsf{MAC}_K(M_\mathrm{B}) \,\big|\, \mathsf{MAC}_{K'}(M_\mathrm{A}) E, M_\mathrm{A} = m_\mathrm{A}, M_\mathrm{B} = m_\mathrm{B}\big) < \lambda + \varepsilon_{m_\mathrm{A}, m_\mathrm{B}}.$$

It now follows that

$$
\begin{aligned}
&p_{\mathsf{guess}}\big(\mathsf{MAC}_K(M_\mathrm{B}) \,\big|\, \mathsf{MAC}_{K'}(M_\mathrm{A})M_\mathrm{A}M_\mathrm{B}E, M_\mathrm{A} \neq M_\mathrm{B}\big) \\
&= \sum_{m_\mathrm{A},m_\mathrm{B}} P_{M_\mathrm{A}M_\mathrm{B}|M_\mathrm{A}\neq M_\mathrm{B}}(m_\mathrm{A},m_\mathrm{B}) \\
&\qquad \cdot p_{\mathsf{guess}}\big(\mathsf{MAC}_K(M_\mathrm{B}) \,\big|\, \mathsf{MAC}_{K'}(M_\mathrm{A})E, M_\mathrm{A} = m_\mathrm{A}, M_\mathrm{B} = m_\mathrm{B}\big) \\
&< \sum_{m_\mathrm{A},m_\mathrm{B}} P_{M_\mathrm{A}M_\mathrm{B}|M_\mathrm{A}\neq M_\mathrm{B}}(m_\mathrm{A},m_\mathrm{B})\,(\lambda + \max_{i\in[t]} \varepsilon_{m_\mathrm{A},m_\mathrm{B},i}) \\
&\leq \lambda + \sum_{m_\mathrm{A},m_\mathrm{B}} P_{M_\mathrm{A}M_\mathrm{B}|M_\mathrm{A}\neq M_\mathrm{B}}(m_\mathrm{A},m_\mathrm{B}) \sum_{i\in[t]} \varepsilon_{m_\mathrm{A},m_\mathrm{B},i} \\
&= \lambda + \sum_{i\in[t]} \sum_{m_\mathrm{A},m_\mathrm{B}} P_{M_\mathrm{A}M_\mathrm{B}|M_\mathrm{A}\neq M_\mathrm{B}}(m_\mathrm{A},m_\mathrm{B})\,\varepsilon_{m_\mathrm{A},m_\mathrm{B},i} \\
&= \lambda + \sum_{i\in[t]} \varepsilon_i \leq \lambda + \sum_{i\in[t]} \varepsilon = \lambda + t\varepsilon.
\end{aligned}
$$

This concludes the proof. □

5 Proofs of Security and Privacy

In this section we show that protocol `AUTH` fulfills the properties listed in Definition 6. First of all, note that it is easy to see from the protocol description that the correctness property is satisfied, we do not elaborate further on this here.

Throughout the proofs, let $E_\circ$ be Eve's quantum side information before executing `AUTH`. E_i, where $i \in \{1,\ldots,4\}$, represents Eve's (quantum) side information after the ith round of communication, and hence includes the communicated random variables up to this ith round. E represents Eve's side information after executing `AUTH`, including Bob's decision to accept or reject (E_4 does not include this decision). Furthermore, like in Section 3.1, we write R_A and R_B etc. for Alice and Bob's respective values for R etc.

Theorem 11 (Security)**.** *If $H_{\min}(X_W|WE_\circ) \geq k_K + q$, then Protocol `AUTH` fulfills the security property defined in Definition 6 with*

$$\delta \leq 3\cdot 2^{-q} + \frac{1}{2}\sqrt{2^q(\lambda + t\,\varepsilon_K)}.$$

In fact, we will prove a slightly stronger statement than the security statement, which will be of use also in the proof of the key privacy statement. Let $M_\mathrm{A} := (\mu_\mathrm{A}, R_\mathrm{A}, S_\mathrm{A})$ and $M_\mathrm{B} := (\mu_\mathrm{B}, R_\mathrm{B}, S_\mathrm{B})$. We will prove that in protocol `AUTH`, if $H_{\min}(X_W|WE_\circ) \geq k_K + q$, and conditioned on the event $M_\mathrm{A} \neq M_\mathrm{B}$, Bob rejects except with probability

$$\delta' \leq 3\cdot 2^{-q} + \frac{1}{2}\sqrt{2^q(\lambda + t\,\varepsilon_K/\Pr[M_\mathrm{A} \neq M_\mathrm{B}])}.$$

Note that this expression reduces to the simpler expression of Theorem 11 when proving security, because in that case $\mu_\mathrm{A} \neq \mu_\mathrm{B}$ (by Definition 6) which implies that $\Pr[M_\mathrm{A} \neq M_\mathrm{B}] = 1$.

Proof. Consider the phase in protocol `AUTH` after the second round of communication. Assume that Z_A and T_A are given to the adversary (this will only make her stronger). Let $K_\mathrm{A} := \mathsf{IaExt}(X_W; R_\mathrm{A})$ and $K_\mathrm{B} := \mathsf{IaExt}(X_W; R_\mathrm{B})$.

From the chain rule, and by subsequently using that R_{B} and S_{A} are sampled independently, it follows that

$$H_{\min}(X_W|Z_{\mathrm{A}}WE_2) \geq H_{\min}(X_W|WE_2) - q \geq H_{\min}(X_W|WE_\circ) - q.$$

By assumption on the parameters, i.e. $H_{\min}(X_W|WE_\circ) \geq k_K + q$, it follows that $(K_{\mathrm{B}}, K_{\mathrm{A}})$ is ε_K-look-ahead conditioned on Z_{A}, W and E_2. In order to apply Lemma 10, we additionally condition on the event $M_{\mathrm{A}} \neq M_{\mathrm{B}}$. By Lemma 2, it is guaranteed that ε_K grows at most by a factor $1/\Pr[M_{\mathrm{A}} \neq M_{\mathrm{B}}]$ as a result of this conditioning. We now apply Lemma 10 and conclude that

$$p_{\mathsf{guess}}(T_{\mathrm{B}}|T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}}) \leq \lambda + t\,\varepsilon_K/\Pr[M_{\mathrm{A}} \neq M_{\mathrm{B}}].$$

The next step is to view $Q_{\mathrm{B}} := [U_{\mathrm{B}} \cdot T_{\mathrm{B}}]_q \oplus V_{\mathrm{B}} \cdot Z_{\mathrm{B}}$ as the output of a strong extractor, with seed $(U_{\mathrm{B}}, V_{\mathrm{B}})$. Indeed, it is straightforward to verify that $h : \{0,1\}^s \times \{0,1\}^q \times \{0,1\}^s \times \{0,1\}^q \to \{0,1\}^q$, which maps (t, z, u, v) to $[u \cdot t]_q \oplus v \cdot z$, is a universal hash function (with random seed (u, v)). Thus, we can apply privacy amplification. One subtlety is that in protocol `AUTH`, V_{B} is random in $\mathbb{F}^*_{2^q}$, rather than in $\mathbb{F}_{2^q}$. Nonetheless, the overall state will be 2^{-q}-close in trace distance to a state where V_{B} would be random over $\mathbb{F}_{2^q}$, and hence, by the triangle inequality, the distance-to-uniform increases by an additive term of at most $2 \cdot 2^{-q}$:

$$\begin{aligned}
&d_{\mathrm{unif}}(Q_{\mathrm{B}}|U_{\mathrm{B}}V_{\mathrm{B}}T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}}) \\
&\qquad \leq \tfrac{1}{2}\sqrt{2^q p_{\mathsf{guess}}(T_{\mathrm{B}}Z_{\mathrm{B}}|T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}})} + 2 \cdot 2^{-q} \\
&\qquad \leq \tfrac{1}{2}\sqrt{2^q p_{\mathsf{guess}}(T_{\mathrm{B}}|T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}})} + 2 \cdot 2^{-q} \\
&\qquad \leq \tfrac{1}{2}\sqrt{2^q(\lambda + t\,\varepsilon_K/\Pr[M_{\mathrm{A}} \neq M_{\mathrm{B}}])} + 2 \cdot 2^{-q}.
\end{aligned}$$

Finally, we have that

$$\begin{aligned}
\delta' &= p_{\mathsf{guess}}\big(Q_{\mathrm{B}}\big|Q_{\mathrm{A}}WE_3, M_{\mathrm{A}} \neq M_{\mathrm{B}}\big) \\
&\leq p_{\mathsf{guess}}\big(Q_{\mathrm{B}}\big|U_{\mathrm{B}}V_{\mathrm{B}}T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}}\big) \\
&\leq 2^{-q} + d_{\mathrm{unif}}(Q_{\mathrm{B}}|U_{\mathrm{B}}V_{\mathrm{B}}T_{\mathrm{A}}Z_{\mathrm{A}}WE_2, M_{\mathrm{A}} \neq M_{\mathrm{B}}) \\
&\leq 3 \cdot 2^{-q} + \tfrac{1}{2}\sqrt{2^q(\lambda + t\,\varepsilon_K/\Pr[M_{\mathrm{A}} \neq M_{\mathrm{B}}])}.
\end{aligned}$$

□

Theorem 12 (Long-Term-Key Privacy)**.** *If $H_{\min}(X_W|WE_\circ) \geq \max(q + k_K, k_Z)$, then Protocol `AUTH` fulfills the long-term-key privacy property defined in Definition 6 with*

$$\varepsilon \leq 6 \cdot 2^{-q} + \sqrt{2^q\big(\lambda + t\,\varepsilon_K\big)} + \varepsilon_K + 2\,\varepsilon_Z.$$

Proof. We first prove that none of the messages exchanged during the protocol leaks information about W. Then, we show that in our protocol Bob's decision on whether to accept or reject neither leaks information about W.

In the first three rounds of `AUTH`, Alice and Bob solely exchange independent randomness, so these rounds trivially leak no information about W. The aim in this part of the proof is to show that the fourth message, $Q = [U \cdot T_{\mathrm{A}}]_q \oplus V \cdot Z$, where T_{A} could depend on W, indeed keeps W private.

Because R_{B} is sampled independently of X_W, and by the chain rule, it follows that $H_{\min}(X_W|WE_1[U_{\mathrm{A}} \cdot T_{\mathrm{A}}]_q) \geq H_{\min}(X_W|WE_\circ) - q$. By assumption on the parameters in the statement of the theorem, i.e. $H_{\min}(X_W|WE_\circ) \geq q + k_Z$, and by the properties of Ext it follows that

$$d_{\mathrm{unif}}(Z_{\mathrm{A}}|WE_2[U_{\mathrm{A}} \cdot T_{\mathrm{A}}]_q) \leq d_{\mathrm{unif}}(Z_{\mathrm{A}}|S_{\mathrm{A}}WE_1[U_{\mathrm{A}} \cdot T_{\mathrm{A}}]_q) \leq \varepsilon_Z.$$

By the fact that U_{B} and V_{B} are sampled independently, the following also holds

$$d_{\mathrm{unif}}(Z_{\mathrm{A}}|WE_3[U_{\mathrm{A}} \cdot T_{\mathrm{A}}]_q) \leq \varepsilon_Z.$$

Then, by security of the one-time pad, by the fact that Eve cannot gain information on W by computing Q_{B}, and by assumption that $\rho_{WE_\circ} = \rho_W \otimes \rho_{E_\circ}$,

$$\tfrac{1}{2}\|\rho_{WE_4} - \rho_W \otimes \rho_{E_4}\|_1 \leq \tfrac{1}{2}\|\rho_{WE_3Q_{\mathrm{A}}} - \rho_W \otimes \rho_{E_3Q_{\mathrm{A}}}\|_1 \leq \varepsilon_Z.$$

This completes the first part of the proof.

It remains to show that Bob's decision to accept or reject cannot leak (a substantial amount of) information about W. To show this, we make the following case distinction. In case $\mu_{\mathrm{A}} \neq \mu_{\mathrm{B}}$, the security proof applies and Bob rejects except with probability $\delta \leq 3 \cdot 2^{-q} + \frac{1}{2}\sqrt{2^q(\lambda + t\,\varepsilon_K)}$. It now immediately follows that

$$\tfrac{1}{2}\|\rho_{WE_4} - \rho_{WE}\|_1 \leq \delta, \quad \text{and} \quad \tfrac{1}{2}\|\rho_W \otimes \rho_{E_4} - \rho_W \otimes \rho_E\|_1 \leq \delta.$$

Hence, in case $\mu_{\mathrm{A}} \neq \mu_{\mathrm{B}}$ (by the triangle inequality),

$$\tfrac{1}{2}\|\rho_{WE} - \rho_W \otimes \rho_E\|_1 \leq \varepsilon_Z + 2\delta.$$

We now turn to the case $\mu_{\mathrm{A}} = \mu_{\mathrm{B}}$ and we analyze for two disjoint events. Conditioned on $M_{\mathrm{A}} \neq M_{\mathrm{B}}$, the strengthened version of the security statement applies, i.e.

$$\delta' \leq 3 \cdot 2^{-q} + \tfrac{1}{2}\sqrt{2^q\big(\lambda + t\,\varepsilon_K/\Pr[M_{\mathrm{A}} \neq M_{\mathrm{B}}]\big)},$$

and again by applying the triangle inequality, we obtain

$$\tfrac{1}{2}\|\rho_{WE|M_{\mathrm{A}} \neq M_{\mathrm{B}}} - \rho_W \otimes \rho_{E|M_{\mathrm{A}} \neq M_{\mathrm{B}}}\|_1 \leq \varepsilon_Z + 2\delta'.$$

Secondly, we analyze for the event $M_{\mathrm{A}} = M_{\mathrm{B}}$. Nevertheless, we start this analysis without conditioning on $M_{\mathrm{A}} = M_{\mathrm{B}}$. (We'll condition on this event later in the proof.) Since S_{A} is sampled at random and independently of X_W, and since $H_{\min}(X_W|WE_\circ) > k_Z$, it follows that

$$d_{\mathrm{unif}}(Z_{\mathrm{A}}|S_{\mathrm{A}}WE_\circ) < \varepsilon_Z\,.$$

By the chain rule (and the independent choice of S_{A}),

$$H_{\min}(X_W|Z_{\mathrm{A}}WE_2) \geq H_{\min}(X_W|WE_\circ) - q > k_K\,,$$

and thus

$$d_{\mathrm{unif}}(K_{\mathrm{B}}|R_{\mathrm{B}}Z_{\mathrm{A}}S_{\mathrm{A}}WE_\circ) < \varepsilon_K\,.$$

From the above, and the independent choices of R_{B} and S_{A}, it follows that

$$\tfrac{1}{2}\|\rho_{K_{\mathrm{B}}Z_{\mathrm{A}}R_{\mathrm{B}}S_{\mathrm{A}}WE_\circ} - \rho_U \otimes \rho_{U'} \otimes \rho_{R_{\mathrm{B}}} \otimes \rho_{S_{\mathrm{A}}} \otimes \rho_W \otimes \rho_{E_\circ}\|_1 \leq \varepsilon_K + \varepsilon_Z.$$

where ρ_U is the fully mixed state on $\mathcal{H}_{K_\mathrm{B}}$ and $\rho_{U'}$ is the fully mixed state on $\mathcal{H}_{Z_\mathrm{A}}$, and therefore that

$$\tfrac{1}{2}\|\rho_{K_\mathrm{B}Z_\mathrm{A}WE_2} - \rho_U \otimes \rho_{U'} \otimes \rho_W \otimes \rho_{E_2}\|_1 \leq \varepsilon_K + \varepsilon_Z.$$

We now condition on $M_\mathrm{A} = M_\mathrm{B}$. Note that conditioned on this event, $K_\mathrm{A} = K_\mathrm{B}$ and $Z_\mathrm{A} = Z_\mathrm{B}$, and therefore, from here on, we omit the subscripts for these random variables and simply write K and Z. From Lemma 2 (noting that whether the event $M_\mathrm{A} = M_\mathrm{B}$ holds is determined by E_2), we get

$$\tfrac{1}{2}\|\rho_{KZWE_2|M_\mathrm{A}=M_\mathrm{B}} - \rho_U \otimes \rho_{U'} \otimes \rho_W \otimes \rho_{E_2|M_\mathrm{A}=M_\mathrm{B}}\|_1 \leq \frac{\varepsilon_K + \varepsilon_Z}{\Pr[M_\mathrm{A} = M_\mathrm{B}]}.$$

U_B and V_B are chosen uniformly at random and independent of the rest (and also independently of the event $M_\mathrm{A} = M_\mathrm{B}$). Furthermore, since E is computed from (KZE_4) alone, it follows that

$$\tfrac{1}{2}\|\rho_{WE|M_\mathrm{A}=M_\mathrm{B}} - \rho_W \otimes \rho_{E|M_\mathrm{A}=M_\mathrm{B}}\|_1 \leq \frac{\varepsilon_K + \varepsilon_Z}{\Pr[M_\mathrm{A} = M_\mathrm{B}]}.$$

We now combine the analyses for the two disjoint events, and conclude that in case $\mu_\mathrm{A} = \mu_\mathrm{B}$,

$$\begin{aligned}
&\tfrac{1}{2}\|\rho_{WE} - \rho_W \otimes \rho_E\|_1 \\
&\quad\leq \Pr[M_\mathrm{A} \neq M_\mathrm{B}]\, \tfrac{1}{2}\|\rho_{WE|M_\mathrm{A}\neq M_\mathrm{B}} - \rho_W \otimes \rho_{E|M_\mathrm{A}\neq M_\mathrm{B}}\|_1 \\
&\qquad\quad + \Pr[M_\mathrm{A} = M_\mathrm{B}]\, \tfrac{1}{2}\|\rho_{WE|M_\mathrm{A}= M_\mathrm{B}} - \rho_W \otimes \rho_{E|M_\mathrm{A}= M_\mathrm{B}}\|_1 \\
&\quad= \Pr[M_\mathrm{A} \neq M_\mathrm{B}]\, (\varepsilon_Z + 2\delta') + \varepsilon_K + \varepsilon_Z \\
&\quad\leq \Pr[M_\mathrm{A} \neq M_\mathrm{B}] \left[\varepsilon_Z + 6\cdot 2^{-q} + \sqrt{2^q\big(\lambda + t\,\varepsilon_K/\Pr[M_\mathrm{A} \neq M_\mathrm{B}]\big)}\right] + \varepsilon_K + \varepsilon_Z \\
&\quad\leq 6\cdot 2^{-q} + \sqrt{2^q\big(\lambda + t\,\varepsilon_K\big)} + \varepsilon_K + 2\,\varepsilon_Z.
\end{aligned}$$

Note that we have computed two upper bounds on $\frac{1}{2}\|\rho_{WE} - \rho_W \otimes \rho_E\|_1$, for two distinct cases: $\mu_\mathrm{A} \neq \mu_\mathrm{B}$ and $\mu_\mathrm{A} = \mu_\mathrm{B}$. Obviously, the weaker (larger) upper bound holds in both cases, and we finally conclude that

$$\tfrac{1}{2}\|\rho_{WE} - \rho_W \otimes \rho_E\|_1 \leq 6\cdot 2^{-q} + \sqrt{2^q\big(\lambda + t\,\varepsilon_K\big)} + \varepsilon_K + 2\,\varepsilon_Z.$$

□

6 Instantiating the Building Blocks

6.1 Look-Ahead Extractors against Classical Side Information

Dodis and Wichs [DW09] propose a construction for look-ahead extractors based on *alternating extraction* [DP07]. The construction uses two strong extractors, which are applied in an alternating fashion (we will explain the construction in detail later in this section). The following theorem due to [DW09] states for this construction how the parameters of the two extractors lead to the parameters of the constructed look-ahead extractor.

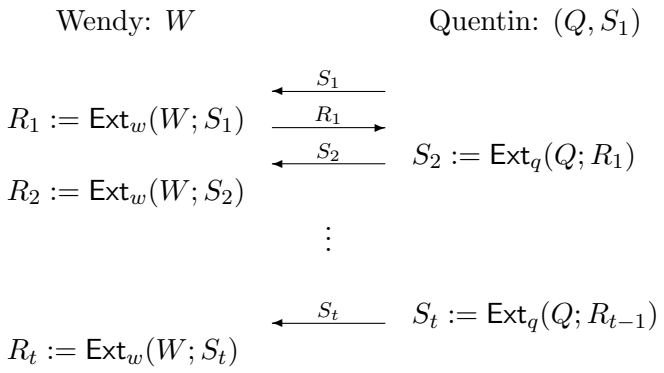

Figure 1: Alternating extraction explained.

The security definition of a look-ahead extractor, Definition 8, considers quantum side information, represented by E. In this section, we consider the case where the side information E is purely classical. To avoid confusion, we will throughout this section write Z (instead of E) for the adversary's *classical* side information. Note that Z has arbitrary range.

Theorem 13 (cf. Theorem 10 in [DW09])**.** *Given an* $(k_w - 2t\ell, \varepsilon_w)$*-extractor* $\mathsf{Ext}_w : \{0,1\}^{n_w} \times \{0,1\}^{\ell} \to \{0,1\}^{\ell}$ *and an* $(n_q - 2t\ell, \varepsilon_q)$*-extractor* $\mathsf{Ext}_q : \{0,1\}^{n_q} \times \{0,1\}^{\ell} \to \{0,1\}^{\ell}$*, the construction in [DW09] yields an* $(k_w, t^2(\varepsilon_w + \varepsilon_q))$*-look-ahead extractor*

$$\mathsf{laExt} : \{0,1\}^{n_w} \times \{0,1\}^{n_q+\ell} \to (\{0,1\}^{\ell})^t$$

Recently, we, and independently, Reyzin [RWY11] discovered that the proof given in [DW09] of Theorem 13 is not fully correct, due to a problem with Lemma 1 in [DP07].[3] Fortunately, the proof (of Theorem 13) could be fixed as shown in lecture notes by Reyzin [RWY11]. In the remainder of this section, we will explain the alternating extraction construction and reprove it for the case in which the side information is classical. Our proof of Theorem 14 (which is then used to prove Theorem 13) is inspired by Reyzin's proof [RWY11], but is more extensive (we consider auxiliary classical side information and we give formal min-entropy analyses, which are omitted in [RWY11]). Furthermore, our proof uses our Lemma 15, which we think is simpler than the corresponding Lemma 6 in [RWY11].

Look-Ahead Extractors from Alternating Extraction

The look-ahead extractor construction is easy to explain. Following [DP07], we identify two parties, Quentin and Wendy. With these parties, we associate the two extractors from Theorem 13, Ext_q and Ext_w, as well as two random variables, $Q \in \{0,1\}^{n_q}$ and $W \in \{0,1\}^{n_w}$, respectively. Quentin and Wendy perform *alternating extraction* as follows (see also Figure 1). Quentin begins by sending a string $S_1 \in \{0,1\}^{\ell}$ to Wendy. Wendy then uses S_1 as seed for her extractor: she computes $R_1 := \mathsf{Ext}_w(W; S_1)$ and sends R_1 back to Quentin. Quentin then uses R_1 as seed and computes $S_2 := \mathsf{Ext}_q(Q; R_1)$, and sends this to Wendy again, etc. The procedure stops after Wendy has computed R_t.

[3] In [DW09], this lemma is called Lemma 31 and is used in the proof of Lemma 41.

The alternating extraction procedure is a construction for the look-ahead extractor in the following way: W is the weakly random source, the tuple $S := (Q, S_1)$ acts as seed, and Wendy's output values $\{R_i\}_{i\in[t]}$ form the output, i.e. $(R_1, \ldots, R_t) = \mathsf{laExt}(W; S)$.

Definition 8 considers *two* instances of a look-ahead extractor: the one at Bob's side[4], which is provided with the original seed, and the one at Alice's side, which is provided with the adversarially modified seed. In terms of our alternating extraction explanation, Quentin and Wendy as described above reside on Bob's side. On Alice's side, we will call the corresponding parties $\widetilde{\text{Q}}$uentin and $\widetilde{\text{W}}$endy. $\widetilde{\text{Q}}$uentin's initial view consists of $(\tilde{Q}, \tilde{S}_1, Z)$ (where $(\tilde{Q}, \tilde{S}_1)$ equals $\tilde{S}$ from Definition 8) and $\widetilde{\text{W}}$endy's initial view consists of (W, Z). $\widetilde{\text{Q}}$uentin and $\widetilde{\text{W}}$endy exchange ℓ-bit messages which we denote as $\tilde{S}_i$ and $\tilde{R}_i$ respectively. These messages are computed from their views in iteration i, which each consist of the party's initial view concatenated with the messages exchanged during alternating extraction.

To prove Theorem 13, we let Quentin and Wendy as well as $\widetilde{\text{Q}}$uentin and $\widetilde{\text{W}}$endy perform alternating extraction *synchronously*. In particular, we need Theorem 14 as an ingredient, which informally states that the ith message produced by Wendy looks random from the combined view of Quentin and $\widetilde{\text{Q}}$uentin, and *vice versa*. Note that the combined view of Quentin and $\widetilde{\text{Q}}$uentin equals the view of the (implicit) adversary in Definition 8.

We will use the following notation for collections of random variables S_i and R_i (as well as $\tilde{S}_i$ and $\tilde{R}_i$),

$$S_{[i]} := (S_1, \ldots, S_i) \quad \forall i \in \mathbb{N} \setminus \{0\},$$

and likewise for $R_{[i]}$, $\tilde{S}_{[i]}$ and $\tilde{R}_{[i]}$. Furthermore, $S_{[i]}$ for any $i < 1$ denotes the empty list, and likewise for $R_{[i]}$, etc.

Theorem 14. *Let ε_q and ε_w as in Theorem 13 and let W, Q, $\tilde{Q}$, S_i, R_i, $\tilde{S}_i$, $\tilde{R}_i$ and Z be as described above. If $P_{S_1QWZ} = P_U P_{U'} P_{WZ}$, where P_U and $P_{U'}$ are uniform distributions on $\{0,1\}^\ell$ and $\{0,1\}^{n_q}$ respectively and if $H_{\min}(W|Z) \geq k_w$, then the following inequalities hold for all $i \in [t]$:*

$$d_{\text{unif}}(S_i | W S_{[i-1]} R_{[i-1]} \tilde{R}_{[i-1]} \tilde{S}_{[i-1]} Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) \tag{1}$$

$$d_{\text{unif}}(R_i | Q R_{[i-1]} S_{[i]} \tilde{R}_{[i-1]} \tilde{S}_{[i]} \tilde{Q} Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w, \tag{2}$$

Note that we require Q to be uniformly distributed; this stems from the parameters of Ext_q, which we adopt from Theorem 13. By adapting the parameters of Ext_q appropriately, alternating extraction also works when Q does not have full min-entropy (cf. [DW09, RWY11]). Nevertheless, since we anyway do not need this more general case, we find it simpler to state it as above.

As in [RWY11], the proof is based on the *conditional independence* of Q and W (when conditioned on the messages exchanged in the alternating-extraction protocol). This independence is crucial for inequalities (1) and (2) to hold because S_i (R_i) is extracted from Q (W) via a seed that is computed from W (Q), and it is well known that for an extractor to work properly the seed must be (essentially) independent from the source.

Consider the general setting where two parties, holding independent random variables X and Y respectively, interact by exchanging messages, where each message is computed

[4] We consider a setting where Alice wants to use the look-ahead extractor to authenticate a message to Bob. Recall that in such a setting Bob samples the seed.

from the sender's random variable (i.e., *either* X or Y) and previously exchanged messages. Then, it is well known (and straightforward to prove) that $X \leftrightarrow M \leftrightarrow Y$ holds, where M represents the collection of the exchanged messages. Observe that alternating extraction (when viewing Wendy and $\widetilde{\text{W}}$endy as a single party and Quentin and $\widetilde{\text{Q}}$uentin as well) is a particular instance of the above general setting. Note that the (classical) side information Z should be treated as being part of M; it can be thought of an initial message that is sent from $\widetilde{\text{W}}$endy to $\widetilde{\text{Q}}$uentin.

To prove Theorem 14 we will use the following lemma, which is a corrected and extended version of Lemma 1 from [DP07].

Lemma 15. *Let A, B, C be arbitrary random variables over respectively $\mathcal{A}, \mathcal{B}, \mathcal{C}$ such that $A \leftrightarrow B \leftrightarrow C$. Then, for any function $f : \mathcal{A} \times \mathcal{C} \to \mathcal{Z}$ it holds that*

$$d_{\text{unif}}(f(A,C)|BC) \leq d_{\text{unif}}(f(A,U)|BU) + d_{\text{unif}}(C|B)$$

where U is an independent random variable uniformly distributed over $\mathcal{C}$.

Proof.

$$\begin{aligned} d_{\text{unif}}(C|B) &= \tfrac{1}{2}\|\rho_{CB} - \rho_U \otimes \rho_B\|_1 \\ &= \tfrac{1}{2}\|\rho_{CBA} - \rho_U \otimes \rho_{BA}\|_1 \\ &\geq \tfrac{1}{2}\|\rho_{f(A,C)BC} - \rho_{f(A,U)BU}\|_1 \end{aligned}$$

where the first equality is by definition of the trace distance to uniform, the second equality follows from the Markov property, and the inequality is by the fact that the trace distance cannot increase under quantum operations. Finally, the claim follows by applying triangle inequality. □

Proof of Theorem 14. We prove the statement by induction on i. Inequality (1) obviously holds for $i = 1$,

$$d_{\text{unif}}(S_i|WS_{[i-1]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z)\big|_{i=1} = d_{\text{unif}}(S_1|WZ) = 0.$$

The first half of the induction step is to show that, if (1) holds for i (the induction hypothesis), then (2) must hold for i, i.e.

$$d_{\text{unif}}(R_i|QR_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}\tilde{Q}Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w.$$

The (trace) distance to uniform cannot increase when applying the same operation to both states (in this case: removing W)

$$\begin{aligned} d_{\text{unif}}(S_i|S_{[i-1]}R_{[i-1]}\tilde{R}_{[i-1]}\tilde{S}_{[i-1]}Z) &\leq d_{\text{unif}}(S_i|WS_{[i-1]}R_{[i-1]}\tilde{R}_{[i-1]}\tilde{S}_{[i-1]}Z) \\ &\leq (\varepsilon_q + \varepsilon_w)(i-1). \end{aligned} \tag{3}$$

The following bound holds on the conditional min-entropy of W,

$$\begin{aligned} H_{\min}(W|S_{[i-1]}R_{[i-1]}\tilde{R}_{[i-1]}\tilde{S}_{[i-1]}Z) &\geq H_{\min}(W|S_{[i-1]}R_{[i-1]}\tilde{R}_{[i-1]}\tilde{S}_{[i-1]}QZ) \\ &= H_{\min}(W|S_1R_{[i-1]}\tilde{R}_{[i-1]}QZ) \\ &\geq H_{\min}(W|S_1QZ) - H_{\max}(R_{[i-1]}\tilde{R}_{[i-1]}) \\ &= H_{\min}(W|Z) - 2(i-1)\ell \\ &\geq k_w - 2(t-1)\ell, \end{aligned}$$

where the first inequality holds by strong subadditivity, the first equality holds because $W \leftrightarrow R_{[i-1]}\tilde{R}_{[i-1]}S_1QZ \leftrightarrow \tilde{S}_{[i-1]}S_{[i-1]} \setminus \{S_1\}$ (which holds because of the way the S_i and $\tilde{S}_i$ are computed), the second inequality is the chain rule and the second equality holds because $P_{WZS_1Q} = P_{WZ}P_UP_Q$. The definition of Ext_w then guarantees that

$$d_{\text{unif}}(\mathsf{Ext}_w(W;U)|US_{[i-1]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z) \leq \varepsilon_w, \tag{4}$$

for an independent and uniform seed U.

Given that $W \leftrightarrow S_{[i-1]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z \leftrightarrow Q$ is a Markov chain (as explained before Lemma 15), it follows that $W \leftrightarrow S_{[i-1]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z \leftrightarrow S_i$ holds as well, since S_i is a function of Q and R_{i-1}. Now, given the latter Markov chain and (3) and (4), we can apply Lemma 15 with $A = W$, $B = S_{[i-1]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z$, $C = S_i$ and $U = U$, which guarantees that

$$d_{\text{unif}}(\mathsf{Ext}_w(W;S_i)|R_{[i-1]}S_{[i]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w.$$

Because it holds that $Q \leftrightarrow S_{[i]}R_{[i-1]}\tilde{S}_{[i-1]}\tilde{R}_{[i-1]}Z \leftrightarrow W$, we may additionally condition on Q in the expression above without increasing the trace distance to uniform. Furthermore, since both $\tilde{Q}$ and $\tilde{S}_i$ can be computed from the random variables that are already being conditioned on, we can also condition on them "for free." Since $R_i := \mathsf{Ext}_w(W;S_i)$ we obtain

$$d_{\text{unif}}(R_i|QR_{[i-1]}S_{[i]}\tilde{Q}\tilde{S}_{[i]}\tilde{R}_{[i-1]}Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w,$$

which is (2) for i and concludes the proof of the first half of the induction step.

The second half of the induction step is to take the expression above as the induction hypothesis and show that if hypothesis is true, then (1) must hold for $i+1$, i.e.

$$d_{\text{unif}}(S_{i+1}|WS_{[i]}R_{[i]}\tilde{S}_{[i]}\tilde{R}_{[i]}Z) \leq (\varepsilon_q + \varepsilon_w)i.$$

This second part is essentially a "mirror image" of the above part.

By an elementary property of the trace distance, the distance to uniform cannot increase when applying a function to both states (it this case: removing systems Q and $\tilde{Q}$):

$$\begin{aligned} d_{\text{unif}}(R_i|R_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z) &\leq d_{\text{unif}}(R_i|QR_{[i-1]}S_{[i]}\tilde{Q}\tilde{S}_{[i]}\tilde{R}_{[i-1]}Z) \\ &\leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w. \end{aligned} \tag{5}$$

The following bound holds on the conditional min-entropy of Q,

$$\begin{aligned} H_{\min}(Q|R_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z) &\geq H_{\min}(Q|WR_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z) \\ &= H_{\min}(Q|WZS_{[i]}\tilde{S}_{[i]}) \\ &\geq H_{\min}(Q|WZS_1) - H_{\max}(\tilde{S}_{[i]}S_{[i]} \setminus \{S_1\}) \\ &= n_q - (2i-1)\ell \\ &\geq n_q - (2t-1)\ell, \end{aligned}$$

where the first inequality holds by strong subadditivity, the first equality holds because $Q \leftrightarrow WZS_{[i]}\tilde{S}_{[i]} \leftrightarrow R_{[i-1]}\tilde{R}_{[i-1]}$, the second inequality is the chain rule, the second equality holds because $P_{WZS_1Q} = P_{WZ}P_UP_{U'}$ and the last inequality follows because $i \leq t$. The definition of Ext_q then guarantees that

$$d_{\text{unif}}(\mathsf{Ext}_q(Q;U)|UR_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z) \leq \varepsilon_q, \tag{6}$$

for an independent and uniform seed U.

Note that from the fact that $Q \leftrightarrow R_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z \leftrightarrow W$, it follows that $Q \leftrightarrow R_{[i-1]}S_{[i]}Z \leftrightarrow R_i$ since R_i is a function of W and S_i. Given this latter Markov chain and (5) and (6), we can apply Lemma 15 with $A = Q$, $B = S_{[i]}R_{[i-1]}\tilde{S}_{[i]}\tilde{R}_{[i-1]}Z$, $C = R_i$ and $U = U$, which guarantees that

$$d_{\text{unif}}(\mathsf{Ext}_q(Q; R_i)|R_{[i]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}Z) \leq (\varepsilon_q + \varepsilon_w)i.$$

Because it holds that $Q \leftrightarrow S_{[i]}R_{[i]}\tilde{S}_{[i]}\tilde{R}_{[i-1]}Z \leftrightarrow W$, we may additionally condition on W without increasing the distance to uniform. Furthermore, we may condition on $\tilde{R}_i$ as well since it is computed as a function of W and $\tilde{S}_i$,

$$d_{\text{unif}}(\mathsf{Ext}_q(Q; R_i)|WR_{[i]}S_{[i]}\tilde{R}_{[i]}\tilde{S}_{[i]}Z) \leq (\varepsilon_q + \varepsilon_w)i.$$

Finally, we obtain (1) for $i + 1$ by noting that $S_{i+1} := \mathsf{Ext}_q(Q; R_i)$ and this proves the second half of the induction step. □

Finally, we prove the main claim. The proof below is essentially the same as the proof of Theorem 9 in [DW09], but then adapted to our notation.

Proof of Theorem 13. We need to prove that

$$d_{\text{unif}}(R_{i+1} \dots R_t|\tilde{R}_{[i]}S\tilde{S}Z) \leq t^2(\varepsilon_q + \varepsilon_w).$$

Note that Definition 8 already requires that S_1 and Q are uniformly distributed and independent of W and Z and that $H_{\min}(W|Z) \geq k_w$, so Theorem 14 applies.

Consider (2) from Theorem 14, i.e.

$$d_{\text{unif}}(R_i|QR_{[i-1]}S_{[i]}\tilde{R}_{[i-1]}\tilde{S}_{[i]}\tilde{Q}Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w,$$

Let us remove the conditioning on $S_{[i]}$ and $\tilde{S}_{[i]}$ except for S_1 and $\tilde{S}_1$, by elementary properties of the trace distance this cannot increase the distance. As mentioned on page 17, $S := (Q, S_1)$ and similarly $\tilde{S} := (\tilde{Q}, \tilde{S}_1)$, so we replace $(Q, S_1, \tilde{Q}, \tilde{S}_1)$ by $(S, \tilde{S})$. Furthermore, we may obviously append independent uniform randomness without increasing the distance-to-uniform:

$$d_{\text{unif}}(R_iU_{\ell(t-i)}|R_{[i-1]}\tilde{R}_{[i-1]}S\tilde{S}Z) \leq (\varepsilon_q + \varepsilon_w)(i-1) + \varepsilon_w, \tag{7}$$

We will evaluate (7) using the substitutions $i \to i + 1$ up to $i \to t$:

$$\begin{aligned}
d_{\text{unif}}(R_{i+1}U_{\ell(t-i-1)}|R_{[i]}\tilde{R}_{[i]}S\tilde{S}Z) &\leq (\varepsilon_q + \varepsilon_w)i + \varepsilon_w,\\
d_{\text{unif}}(R_{i+2}U_{\ell(t-i-2)}|R_{[i+1]}\tilde{R}_{[i+1]}S\tilde{S}Z) &\leq (\varepsilon_q + \varepsilon_w)(i+1) + \varepsilon_w,\\
&\vdots\\
d_{\text{unif}}(R_t|R_{[t-1]}\tilde{R}_{[t-1]}S\tilde{S}Z) &\leq (\varepsilon_q + \varepsilon_w)(t-1) + \varepsilon_w.
\end{aligned}$$

By recursively applying the triangle inequality to these expressions (a "hybrid argument") we may conclude that

$$d_{\text{unif}}(R_{i+1} \dots R_t|R_{[i]}\tilde{R}_{[i]}S\tilde{S}Z) \leq \tfrac{1}{2}t(t-1)(\varepsilon_q + \varepsilon_w) + (t-1)\varepsilon_w \leq t^2(\varepsilon_q + \varepsilon_w)$$

Finally, we obtain the claim simply by removing the conditioning on $\tilde{R}_{[i]}$[5]. □

[5] we thus actually prove a slightly stronger statement, i.e. that the claim still holds when conditioning additionally on $R_{[i]}$

Parameters of an Explicit Look-Ahead Extractor

Dodis and Wichs use the explicit strong extractor from [GUV09] to instantiate the extractor in Theorem 13, and achieve the following parameters.

Theorem 16 (Theorem 11 in [DW09])**.** *For all integers $n \geq k$ and all $\varepsilon > 0$ there exist (k, ε)-look-ahead extractors $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to (\{0,1\}^\ell)^t$ as long as*

$$\begin{aligned} k &\geq 2(t+2)\max(\ell, O(\log(n) + \log(t) + \log(1/\varepsilon))) \\ &\geq O(t(\ell + \log(n) + \log(t) + \log(1/\varepsilon))), \end{aligned}$$

and $d \geq O(t(\ell + \log(n) + \log(t) + \log(1/\varepsilon)))$.

I.e., when neglecting logarithmic terms, k and d are both of order $t\ell$, the bit-size of the range of the extractor.

6.2 Look-Ahead Extractors and Quantum Side Information?

In a preliminary version of this paper presented at *Eurocrypt* [BF11], we claimed that one can obtain a look-ahead extractor that is secure against *quantum* side information simply by replacing the classical strong extractors in the original construction by extractors against quantum side information, and furthermore that the original proof strategy can also be used in the quantum setting. Unfortunately, we recently noticed that we have overlooked a subtle issue that renders the original proof strategy invalid for the quantum case. Although the alternating-extraction construction *could* still work in the quantum setting, we currently do not have a proof for it. We leave it as an important open problem.

Let us briefly explain here why the proof strategy for the classical setting does not apply in the quantum setting. Recall that according to Definition 8 the adversary creates $\tilde{S} = (\tilde{Q}, \tilde{S}_1)$ given $S = (Q, S_1)$ and E, and that this process may involve a measurement on E, which then collapses to the state E'. This latter state E' may in particular include Q, and it typically depends on W as well. It is not clear how to generalize Lemma 15 to include this quantum side information. Moreover, the proof for the classical case makes statements about a probability space in which Z and $\tilde{S}$, which is computed from Z, exist simultaneously. In the quantum setting, however, the *original* quantum state E does not exist anymore after it is measured (to produce $\tilde{S}$); it collapses to the post-measurement state E', which is not guaranteed to have the necessary properties (like independence of Q).

6.3 Security and Instantiation of the MAC

To construct a MAC with look-ahead security, we adopt the construction given in [DW09]. Because our look-ahead security definition, Definition 9, is slightly weaker than the one given in [DW09] (in that both μ_A and μ_B are fixed), we obtain a better security parameter, as argued below.

With respect to a different aspect, the requirement on the MAC for constructing our protocol `AUTH` is somewhat stronger, because we need a "universal" MAC which is $(\epsilon, \lambda + \epsilon)$-look-ahead secure *for any* $\epsilon \geq 0$ (and some λ). (This requirement stems from the proof of Lemma 10.) It turns out that the construction from [DW09] satisfies this property.

Proposition 17. *For any positive integers m and ℓ, there exists a family of functions $\{\mathsf{MAC}_\kappa : \{0,1\}^m \to \{0,1\}^s\}$, indexed by keys $\kappa \in (\{0,1\}^\ell)^t$, that is $(\varepsilon, 2^{-\ell} + \varepsilon)$ look-ahead secure for any $\varepsilon > 0$, where $t = 4m$ and $s = 2m\ell$.*

For completeness, we very briefly describe the idea of the construction here. The function $\mathsf{MAC}_\kappa(\mu)$ outputs some of the blocks κ_i of the key $\kappa = (\kappa_1, \ldots, \kappa_t)$; where the choice of this subset is determined by μ. Furthermore, the construction guarantees that for any two distinct messages μ and μ', there exists an index $i_\circ < t$ such that $\mathsf{MAC}_\kappa(\mu)$ outputs more blocks κ_i with $i > i_\circ$ than $\mathsf{MAC}_\kappa(\mu')$ does. From the look-ahead property, it follows that given $\kappa'_1, \ldots, \kappa'_{i_\circ}$, the remaining blocks $\kappa_{i_\circ+1}, \ldots, \kappa_t$ are (ε-close to) random. Then, from the choice of $i_\circ$ and from the chain rule we conclude that when given $\mathsf{MAC}_{\kappa'}(\mu')$, the tag $\mathsf{MAC}_\kappa(\mu)$ still contains at least (nearly) ℓ bits of min-entropy.

Since the security of the MAC follows more or less directly from the look-ahead property (and an application of the chain rule), this construction is secure in the presence of quantum side information when the underlying look-ahead extractor is secure against quantum side information.

When comparing our Proposition 17 with Lemma 15 in Appendix E.3 of [DW09], our modification of fixing both μ_A and μ_B before executing `DWMAC` overcomes the need for a union bound over all possible messages μ_B and hence saves us a factor of 2^m.

6.4 Instantiating Protocol AUTH

We will instantiate protocol `AUTH` for the case of classical side information. Before doing so, we first need to slightly modify the protocol. Because the alternating-extraction construction that we use to instantiate laExt requires a relatively large seed, we cannot let Alice authenticate the tuple (μ_A, R, S) directly. Instead, Alice will sample a seed and for an almost universal hash function, and authenticates the seed and the hash of (μ_A, R, S). We will make use of the well-known polynomial construction for an almost universal hash function (see e.g. [TSSR10]); for some field $\mathbb{F}$ and b a positive integer, let

$$\begin{array}{rccc} h: & \mathbb{F}^b \times \mathbb{F} & \to & \mathbb{F} \\ & (x_1, \ldots, x_b; \alpha) & \mapsto & \sum_{i=1}^b x_i \alpha^{b-i}. \end{array}$$

For α, the seed, randomly chosen from $\mathbb{F}$, the probability that two distinct inputs $x, x' \in \mathbb{F}^b$ collide is $p_\mathsf{col} := (b-1)/|\mathbb{F}|$.

This hashing-modification to `AUTH` will affect its security and privacy. We take care of this simply by adding p_col to the security and $2\,p_\mathsf{col}$ to the privacy upper bound. The latter factor of two comes from the triangle inequality, which appears because privacy (as defined in Definition 6) is a distance between two states.

We now combine Theorem 11, Theorem 12, Theorem 16 and Proposition 17 and make use of the hashing modification explained above in order to obtain a lower bound on k, the min-entropy required by `AUTH`, in terms of desired security and privacy parameters and the bitsize of the message to be authenticated.

Corollary 18. *For any integers $n \geq k$, m and any $\varepsilon > 0$ and any $0 < \delta \leq \varepsilon/8$, we can construct an efficient four-round $(n, k, m, \delta, \varepsilon)$ message-authentication protocol with long-term-key privacy as long as (asymptotically)*

$$k = O\Big(\log(1/\varepsilon) + \big(\log(1/\delta) + \log(m')\big) \cdot \big(\log(1/\delta) + \log(m') + \log(n)\big)\Big),$$

where

$$m' = m + O\Big(\log(1/\varepsilon) + \big(\log(1/\delta) + \log(m')\big) \cdot \big(\log(1/\delta) + \log(m') + \log(n)\big)\Big).$$

Proof. We start by computing suitable parameters for the almost universal hash function. Let $\mathbb{F} := \mathrm{GF}(2^c)$ for a positive integer c, and let m' be the bitsize of the tuple (μ, R, S), i.e. $m' = m + d + v$. Hence, $b = m'/c$,[6] and $p_{\mathsf{col}} = 2^{-c}(m'/c - 1) \leq 2^{-c}\, m'$.

As required by the security and privacy proofs, $k > \max(q + k_K, k_Z)$. We first analyze k_K. Let $\delta' := 3 \cdot 2^{-q} + \frac{1}{2}\sqrt{2^q(2^{-\ell} + t\,\varepsilon_K)} + 2^{-c}\, m'$ (this expression originates from combining Theorem 11, Proposition 17 and p_{col}). To simplify matters, we choose $q = \ell/2$, $c = \ell/2 + \log m'$ and $\varepsilon_K = 2^{-\ell}/t$ and we obtain

$$\begin{aligned}\delta' &= 3 \cdot 2^{-\ell/2} + \frac{1}{2}\sqrt{2^{\ell/2}(2 \cdot 2^{-\ell})} + 2^{-(\ell/2 + \log m')}\, m' \\ &= 3 \cdot 2^{-\ell/2} + 2^{-\frac{1}{2} - \frac{\ell}{4}} + 2^{-\ell/2} \lessapprox 2^{-\ell/4} \quad \text{(for large enough } \ell\text{)}.\end{aligned}$$

Because δ' is an upper bound for the security of `AUTH`, a sufficient condition to achieve the desired security level δ is when $\delta' \leq \delta$. Hence, we choose

$$\ell \geq 4 \log(1/\delta).$$

The actual message to be authenticated consists of the seed and the hash value and therefore has bit-length $2c$. Then, by Proposition 17 we have that $t = 4(2c) = 4\ell + 8 \log m' \geq 16 \log(1/\delta) + 8 \log m'$. We substitute this into the expression for ε_K:

$$\varepsilon_K \leq \delta^4/(16 \log(1/\delta) + 8 \log m').$$

Next, we plug this into the bound for k from Theorem 16. This yields

$$k_K = O\Big(\big(\log(1/\delta) + \log(m')\big) \cdot \big(\log(1/\delta) + \log(m') + \log(n)\big)\Big).$$

We now analyze k_Z. Let

$$\begin{aligned}\varepsilon' &:= 6 \cdot 2^{-q} + \sqrt{2^q(2^{-\ell} + t\,\varepsilon_K)} + \varepsilon_K + 2\,\varepsilon_Z + 2^{-c+1} m' \\ &= 2\delta' + \delta'^4/t + 2\varepsilon_Z + 2^{-c+1} m'\end{aligned}$$

be the upper bound on the privacy of `AUTH` (the expression follows from combining Theorem 12, Proposition 17 and p_{col}). To achieve the desired privacy ε, it suffices that $\varepsilon' \leq \varepsilon$. By substituting $\delta' = \delta$ and solving for ε_Z, we obtain $\varepsilon_Z \leq \frac{1}{2}\varepsilon - \delta - \frac{1}{2t}\delta^4 - 2^{-\ell/2} \leq \frac{1}{2}\varepsilon - \delta - \frac{1}{2t}\delta^4 - \delta^2$. From the latter expression, we see why we cannot choose δ arbitrarily large, compared to ε, because an upper bound for ε_Z should of course not be negative. Note that this parameter-dependency is not surprising; it stems from the fact that the privacy proof makes use of the security proof. Therefore, we choose $0 < \delta \leq \varepsilon/8$, such that $\varepsilon_Z \leq \frac{\varepsilon}{2} - \frac{\varepsilon}{8} - \frac{\varepsilon^4}{2^{13} t} - \frac{\varepsilon^2}{64}$. Lower bounding the RHS yields the simpler expression

$$\varepsilon_Z \leq \varepsilon/4.$$

Substituting this into the bound for k from Theorem 16 gives

$$k_Z = O\big(\log(1/\delta) + \log(n) + \log(1/\varepsilon)\big)$$

[6] Here, we assume that m' is an integer multiple of c. Note that this can always be achieved by zero-padding m'.

We upper-bound $\max(q + k_K, k_Z)$ by the sum $q + k_K + k_Z$:

$$\begin{aligned} k &\geq 2\log 1/\delta + k_K + k_Z \\ &= O\Big(\log(1/\varepsilon) + \big(\log(1/\delta) + \log(m')\big) \cdot \big(\log(1/\delta) + \log(m') + \log(n)\big)\Big). \end{aligned}$$

Remember that $m' = (m+d+v)$, where $v = O\big(\log(n)+\log(1/\varepsilon_Z)\big) = O\big(\log(n)+\log(1/\varepsilon)\big)$ and

$$d = O\Big(\big(\log(1/\delta) + \log(m')\big) \cdot \big(\log(1/\delta) + \log(m') + \log(n)\big)\Big).$$

□

7 The Fuzzy Case

Up to here, we assumed a scenario where Alice and Bob share *identical* copies of the session key X_W. Let us now consider the "fuzzy" case, where Alice and Bob hold keys that are only close in some sense, but not necessarily equal. This kind of scenario naturally arises when Alice and Bob obtain their session keys in the presence of noise. For simplicity and with our application (Section 8) in mind, we use the Hamming distance to measure closeness between keys.

Consider the following simple approach. Let Bob's key be called X_W. Before executing the authentication protocol, Bob sends some error-correcting information (like the syndrome of X_W with respect to some error-correcting code) to Alice, so that she can correct the errors in her key, X'_W. Since Eve has full control over the communication channel, she can also modify this error-correction information. In this case Alice might not correct X'_W successfully, in which case our protocol is not guaranteed to be secure. However, as stated in Theorem 22 in [DW09], this approach is secure (in the classical setting) if one uses alternating-extraction-based instantiations of look-ahead extractors. (Note that the parameters change slightly compared to the non-fuzzy case, to take into account the min-entropy loss due to the error correction information.) For this solution to work it is important that X_W has sufficient min-entropy when given Eve's (classical) side information, and that Bob sends the error-correcting information to Alice (i.e. the error-correction information must be sent in the same direction as the seed for the look-ahead extractor).

Because we currently do not have a provably secure construction for a look-ahead extractor against quantum side information, we cannot say whether the approach above also works in the setting where Eve is allowed to have quantum side information. This remains an open question that needs to be solved before protocol `AUTH` can be used to improve the quantum protocol $\texttt{QID}^+$.

One subtlety is that the error-correcting information must not leak information about W, to preserve the privacy property. Exactly this problem is addressed in [DS05], and is generalized to the quantum setting in [FS09]. Note that it is straightforward to upper bound the min-entropy loss in X_W due to error correction: by the chain rule this is at most the bitsize of the error-correction information.

Finally, we want to make a remark about how this min-entropy loss (caused by sending the error-correction information) is incorporated in the parameters of Theorem 22 in [DW09]: Ext_q needs to be an $(n_q - (2\ell + \alpha)t, \varepsilon_q)$-extractor,[7] where α is the bitsize of the

[7] For comparison: in Theorem 13, the non-fuzzy case, Ext_q is a $(n_q - 2\ell t, \varepsilon_q)$-extractor.

error-correction information. In words, there is a loss of αt in the first parameter, where one would expect only a loss of α. To us it seems that the factor t in front of α is not necessary; it is merely a consequence of the proof strategy of Theorem 22, which uses the alternating-extraction theorem (Theorem 9 in [DW09]) as a black box.

Furthermore, it seems that the requirement on the conditional min-entropy of W_A in Theorem 22 (from [DW09]) is not necessary; it is also not used in the proof.

8 Application: Password-Based Identification

We sketch here how an instantiation of protocol AUTH that a) is secure when Eve has quantum side information about the weak key, and b) is still secure in the fuzzy case, would lead to a truly password-based identification protocol in the bounded quantum storage model with security against man-in-the-middle attacks. We want to stress that to achieve a) and to be able to verify b), we still miss one building block, i.e. look-ahead extractors against quantum side information. Damgård *et al.* proposed in [DFSS07] two password-based identification schemes, QID and $\texttt{QID}^+$. The former is truly password based but does not protect against a man-in-the-middle attack, whereas the latter is secure against a man-in-the-middle attack but is not truly password-based, because the "user" U and "server" S need to additionally share a secret high-entropy key.[8] This high-entropy key in $\texttt{QID}^+$ is used to authenticate all classical communication by means of an extractor MAC.

Our idea of obtaining security against man-in-the-middle attacks without a high-entropy key is now simply to do the authentication of the classical communication by applying protocol AUTH when using $x_{\mathcal{I}_w}$ as weak session key. Our privacy property guarantees that the authentication does not leak information on the password w. We stress that previous protocols for authentication based on weak keys would (potentially) leak here information on w.

If the quantum communication is noisy (which it is in realistic scenarios) or if the man-in-the-middle attacker modifies some of the qubits (but few enough so that he is not detected) or θ, then U's and S's version of $x_{\mathcal{I}_w}$ are not identical. Thus, we indeed require that AUTH is secure in the fuzzy case.

If the analysis of the fuzzy case for the case of classical side information would more or less directly carry over to the quantum setting, then this would mean that we need a lower bound on the min-entropy of S's version of $x_{\mathcal{I}_w}$ (when given the adversary's side information). Although the analysis of Damgård *et al.* only guarantees min-entropy in U's version, we can slightly modify the protocol to also guarantee lower-bounded min-entropy on S's side. Instead of measuring the BB84 qubits in basis $c(w)$, S measures them in a *random* basis $\hat{\theta}$ and announces the difference $r = c(w) \oplus \hat{\theta}$. Then, U and S update the code c by shifting every code word by r, so that with respect to the updated code c', S has actually measured the BB84 qubits in basis $c'(w)$. This trick has also been used in [DFL^+09], though for a different reason, and has no real effect on the analysis of the protocol. However, since S now also measures in a random basis, we can apply the

[8] The high entropy key is only needed to protect against a man-in-the-middle attack, security against dishonest U and S only relies on the password and holds even if the dishonest party knows the high entropy key.

uncertainty relation of [DFR+07] to get a lower bound on the min-entropy on S's side.

9 Open Problem

The main open problem of this chapter is showing the existence of (efficient) look-ahead extractors that are secure against quantum side information, by means of coming up with an efficient construction. It remains possible that the alternating-extraction construction also works against quantum side information, but it might also be the case that totally different techniques are needed.

Acknowledgment

We would like to thank Krzysztof Pietrzak for interesting discussions and valuable comments regarding this work.

References

[BF11] Niek J. Bouman and Serge Fehr. Secure authentication from a weak key, without leaking information. In Kenneth Paterson, editor, *Eurocrypt*, volume 6632 of *Lecture Notes in Computer Science*, pages 246–265. Springer, 2011. ePrint:2011/034.

[CKOR10] Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. In *STOC*, pages 785–794. ACM, 2010.

[CW77] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. In *STOC*, pages 106–112, New York, 1977. ACM.

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In *CRYPTO*, Lecture Notes in Computer Science, pages 408–427. Springer, 2009. arXiv:0902.3918.

[DFR+07] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *CRYPTO*, Lecture Notes in Computer Science, pages 360–378. Springer, 2007. arXiv:quant-ph/0612014.

[DFSS07] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and qkd in the bounded-quantum-storage model. In *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007. arXiv:0708.2557.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008. ePrint:2003/235.

[DP07] Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *FOCS*, pages 227–237. IEEE Computer Society, 2007. ePrint:2007/359.

[DS05] Yevgeniy Dodis and Adam Smith. Correcting errors without leaking partial information. In *STOC*, pages 654–663. ACM, 2005.

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *STOC*, pages 601–610, 2009. ePrint:2008/503.

[FS09] Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference - TCC 09*, volume 5444 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2009. arXiv:0804.1059.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *J. ACM*, 56(4), 2009.

[KR09] Bhavana Kanukurthi and Leonid Reyzin. Key agreement from close secrets over unsecured channels. In Antoine Joux, editor, *Eurocrypt*, volume 5479 of *Lecture Notes in Computer Science*, pages 206–223. Springer, 2009. ePrint:2008/494.

[KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Tran. Inf. Th.*, 55(9):4337–4347, 2009. arXiv:0807.1338.

[Mau90] Ueli M. Maurer. A provably-secure strongly-randomized cipher. In *Eurocrypt*, Lecture Notes in Computer Science, pages 361–373. Springer, 1990.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich (Switzerland), September 2005. arXiv:quant-ph/0512258.

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005. arXiv:quant-ph/0403133.

[RW03] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 78–95. Springer, August 2003.

[RW04] Renato Renner and Stefan Wolf. The exact price for unconditionally secure asymmetric cryptography. In Christian Cachin and Jan Camenisch, editors, *Eurocrypt*, volume 3027 of *Lecture Notes in Computer Science*, pages 109–125. Springer, 2004.

[RWY11] Leonid Reyzin, Drew Wolpert, and Sophia Yakoubov. Alternating extractors and leakage-resilient stream ciphers. 6.889 New Developments in Cryptography (lecture notes), `http://www.cs.bu.edu/~reyzin/teaching/s11cs937/notes-leo-2.pdf`, 2011.

[TSSR10] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Tran. Inf. Th.*, 2010. arXiv:1002.2436.

[VDG98] Jeroen Van De Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Univ. de Montreal (Quebec, Canada), 1998.